Network Management & Monitoring

Introduction to SNMP
Overview

- What is SNMP?
- OIDs
- MIBs
- Polling and querying
- Traps
- SNMPv3 (Optional)
What is SNMP?

SNMP – Simple Network Management Protocol
- Industry standard, hundreds of tools exist to exploit it
- Present on any decent network equipment

Query – response based: **GET / SET**
- GET is mostly used for monitoring

Tree hierarchy
- Query for “Object Identifiers” (OIDs)

Concept of MIBs (Management Information Base)
- Standard and vendor-specific (Enterprise)
What is SNMP?

UDP protocol, port 161

Different versions

  - Original specification
- v2 – RFC1901 ... RFC1908 + RFC2578
  - Extends v1, new data types, better retrieval methods (GETBULK)
  - Used is version v2c (without security model)
- v3 – RFC3411 ... RFC3418 (w/security)

Typically we use SNMPv2 (v2c)
What is SNMP?

Terminology:
- Manager (the monitoring "client")
- Agent (running on the equipment/server)
What is SNMP?

Typical queries
- Bytes In/Out on an interface, errors
- CPU load
- Uptime
- Temperature or other vendor specific OIDs

For hosts (servers or workstations)
- Disk space
- Installed software
- Running processes
- ...

Windows and UNIX have SNMP agents
How does it work?

Basic commands

- GET (manager -> agent)
  - Query for a value

- GET-NEXT (manager -> agent)
  - Get next value (list of values for a table)

- GET-RESPONSE (agent -> manager)
  - Response to GET/SET, or error

- SET (manager -> agent)
  - Set a value, or perform action

- TRAP (agent -> manager)
  - Spontaneous notification from equipment (line down, temperature above threshold, ...)

The MIB Tree

root
- ccitt(0)
- iso(1)
- joint-iso-ccitt(3)
- org(3)
- dod(6)
- internet(1)
  - directory(1)
  - mgmt(2)
  - experimental(3)
  - mib-2(1)
    - system(1)
    - interfaces(2)
    - ip(4)
  - private(4)
    - enterprises(1)
    - cisco(9)

1.3.6.1
The MIB Tree

- root
  - ccitt(0)
  - iso(1)
    - joint-iso-ccitt(3)
    - org(3)
      - dod(6)
        - internet(1)
          - directory(1)
          - mgmt(2)
          - experimental(3)
          - mib-2(1)
            - system(1)
            - interfaces(2)
            - snmp(11)
            - ip(4)
          - private(4)
            - enterprises(1)
            - cisco(9)
  - experimental(3)
    - private(4)
      - cisco(9)
      - ciscoMgmt(9)
      - ciscoEnvMonMIB(13)
      - ciscoEnvMonObjects(1)
      - ciscoEnvMonTemperatureStatusTable(3)
      - ciscoEnvMonTemperatureStatusEntry(1)
      - ciscoEnvMonTemperatureStatusValue(3)
      - ...

- mib-2(1)
If email addresses were OIDs...

user@nsrc.org

would have been something like:

user@nsrc.enterprises.private.internet.dod.org.iso

user@99999.1.4.1.6.3.1

except that we write the top-most part at the left:

1.3.6.1.4.1.99999.117.115.101.114

An OID is just a unique key (within one managed device) for one piece of information

Ensures vendors don't have conflicting OIDs
The Internet MIB

• **directory**(1) OSI directory
• **mgmt**(2) RFC standard objects
• **experimental**(3) Internet experiments
• **private**(4) Vendor-specific
• **security**(5) Security
• **snmpV2**(6) SNMP internal
OIDs and MIBs

- Navigate tree downwards
- OIDs separated by '.'
  - 1.3.6.1.4.1.9. ...
- OID corresponds to a label
  - 1.3.6.1.2.1.1.5 => sysName
- The complete path:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName

- How do we convert from OIDs to Labels (and vice versa?)
  - Use of MIBs files!
MIBs

- MIBs are files defining the objects that can be queried, including:
  - Object name
  - Object description
  - Data type (integer, text, list)

- MIBS are structured text, using ASN.1

- Standard MIBs include:
  - MIB-II – (RFC1213) – a group of sub-MIBs
  - HOST-RESOURCES-MIB (RFC2790)
MIBs - 2

MIBs also make it possible to interpret a returned value from an agent

– For example, the status for a fan could be 1,2,3,4,5,6 – what does it mean?
sysUpTime OBJECT-TYPE
SYNTAX  TimeTicks
ACCESS  read-only
STATUS  mandatory
DESCRIPTION
"The time (in hundredths of a second) since the
network management portion of the system was last
re-initialized."
::= { system 3 }

This defines the object called sysUpTime.

SYNTAX TimeTicks
This object is of the type TimeTicks. Object types are specified in the SMI we mentioned a moment ago.

ACCESS read-only
This object can only be read via SNMP (i.e., get-request); it cannot be changed (i.e., set-request).

STATUS mandatory
This object must be implemented in any SNMP agent.

DESCRIPTION
A description of the object

::= { system 3 }
The sysUpTime object is the third branch off of the system object group tree.
CiscoEnvMonState ::= TEXTUAL-CONVENTION
   STATUS  current
   DESCRIPTION
       "Represents the state of a device being monitored. Valid values are:
       normal(1): the environment is good, such as low temperature.
       warning(2): the environment is bad, such as temperature above normal operation range but not too high.
       critical(3): the environment is very bad, such as temperature much higher than normal operation limit.
       shutdown(4): the environment is the worst, the system should be shutdown immediately.
       notPresent(5): the environmental monitor is not present, such as temperature sensors do not exist.
       notFunctioning(6): the environmental monitor does not function properly, such as a temperature sensor generates a abnormal data like 1000 C."
Querying SNMP agent

Some typical commands for querying:

- `snmpget`
- `snmpwalk`
- `snmpstatus`
- `snmpstable`

Syntax:

```
snmpXXX -c community -v1 host [oid]
```

```
snmpXXX -c community -v2c host [oid]
```
Querying SNMP agent

Let's take an example

- `snmpstatus -c NetManage -v2c 10.10.0.254`
- `snmpget -c NetManage -v2c 10.10.0.254 .iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber.0`
- `snmpwalk -c NetManage -v2c 10.10.0.254 ifDescr`
Querying SNMP agent

Community:

– A "security" string (password) to define whether the querying manager will have RO (read only) or RW (read write) access
– This is the simplest form of authentication in SNMP

OID

– A value, for example, .1.3.6.1.2.1.1.5.0, or it's name equivalent
– .iso.org.dod.internet.mgmt.mib-2.system.sysName.0

Let's ask for the system's name (using the OID above)

– Why the .0? What do you notice?
Coming up in our exercises...

- Using snmpwalk, snmpget
- Configuring SNMPD
- Loading MIBs
- Configuring SNMPv3 (optional)
References

• *Essential SNMP* (O’Reilly Books) Douglas Mauro, Kevin Schmi
• *Basic SNMP at Cisco*
• Wikipedia:
• IP Monitor MIB Browser
  http://support.ipmonitor.com/mibs_byoidtree.aspx
• Open Source Java MIB Browser
  http://www.kill-9.org/mbrowse
  http://www.dwipal.com/mibbrowser.htm (Java)
• SNMP Link – collection of SNMP resources
  http://www.snmplink.org/
• Net-SNMP Open Source SNMP tools
  http://net-snmp.sourceforge.net/
• Integration with Nagios http://www.cisl.ucar.edu/nets/tools/nagios/SNMP-traps.html
Optional Materials

SNMP Version 3
SNMP and Security

• SNMP versions 1 and 2c are insecure
• SNMP version 3 created to fix this

• Components
  – Dispatcher
  – Message processing subsystem
  – Security subsystem
  – Access control subsystem
SNMP version 3 (SNMPv3)

The most common module is based in user, or a “User-based Security Model”

- **Authenticity and integrity**: Keys are used for users and messages have digital signatures generated with a hash function (MD5 or SHA)
- **Privacy**: Messages can be encrypted with secret-key (private) algorithms (DES)
- **Temporary validity**: Utilizes a synchronized clock with a 150 second window with sequence checking.
Security Levels

noAuthPriv
   – No authentication, no privacy

authNoPriv
   – Authentication with no privacy

authPriv
   – Authentication with privacy
Cisco SNMPv3 configuration

snmp-server view vista-ro internet included
snmp-server group ReadGroup v3 auth read vista-ro
snmp-server user admin ReadGroup v3 auth md5 xk122r56

Or alternatively:

snmp-server user admin ReadGroup v3 auth md5 xk122r56
  priv des56 D4sd#rr56
# apt-get install snmp snmpd
# net-snmp-config --create-snmpv3-user -a "xk122r56" admin
/usr/sbin/snmpd
# snmpwalk -v3 -u admin -l authNoPriv -a MD5 -A "xk122r56" 127.0.0.1